C1 cont

(c) at each of a plurality of the distributed electronic devices, generating a partial result for the distributed cryptographic computation using at least one of said random values; and

(d) computing a final result for the distributed cryptographic computation using partial results.

REMARKS

The applicants respectfully request reconsideration and allowance of this application. After entry of this Amendment, claims 1-12 and 17-25 will be pending, with claim 1 amended.

Claims 1-12 and 17-31 were rejected as being anticipated by Gennaro et al. For convenience, the applicants respectfully repeat here a short portion of remarks from the Preliminary Amendment with reference to an embodiment disclosed in pages 9-12 of the specification. That embodiment may be implemented in an architecture shown in Fig. 1. For clarity in communicating concepts, shared randomness was discussed with reference to a specific example of distributed signing. Such specificity is not intended to limit the scope of protection.

> Fig. 1 shows an architecture having five signing units. Those devices may be designated as "1," "2," "3," "4," and "5." During a setup phase, members of the system adopt a series of pseudorandom functions $PRF_k(\cdot)$ indexed by variable "k." During later phases, the variable "k" may take on specific values depending on context. Also during the setup phase, each pair of signing devices jointly generates a shared secret key $\sigma_{i,j}$. For example, signing devices "1" and "2" both generate the same shared key $\sigma_{1,2}$ (which is identical to $\sigma_{2,1}$), signing devices "1" and "3" generate a different shared key $\sigma_{1,3}$ and so on for all pairs that can be formed among the five devices. The values of σ may be used as the index value "k" for the pseudorandom function.
>
> During an operation to sign a specific message m, a subset of devices may be selected, such as three out of the five. If the three devices are "1," "2," and "3," the set $\Lambda = \{1, 2, 3\}$. As described on page 11 of the specification, each member of the set Λ will compute a value $s'_{m,j,\Lambda}$ that includes the following term: $\sum v \epsilon \Lambda / j \text{ sign}(j - v) \bullet$

$PRF\sigma_{j,v}$. The sum is taken over all devices v that are elements of the set Λ excluding device j. For signing device "1," j = 1, and the summation has two terms: a term for v = 2 and a term for v = 3. The terms of the summation would be:

$$\text{sign}(1 - 2) \bullet PRF\ \sigma_{1,2}\ (m) + \text{sign}(1 - 3) \bullet PRF\ \sigma_{1,3}.(m).$$

Signing device "2" would have terms for j = 2 and v = 1 , 3. Signing device "3" would have terms for j = 3 and v = 1, 2.

Each pair of signing devices shares a unique source of randomness in the form of the function PRF $\sigma_{j,v}$. Because $\sigma_{j,v} = \sigma_{v,j}$ (they are equal values), pair members will select the same pseudo random function ($PRF\sigma_{j,v} = PRF\sigma_{v,j}$) and contribute partial results with "random" contributions that are actually related to one another. An error or misbehavior of a participant will be revealed if contributions do not relate properly. For example, a final signature will not verify unless both members of a pair contribute shared random values with the required relationship. As stated on page 10 of the specification, the sharing of the pseudorandom functions and their invocation in the computation generates a "t-wise hand shake."

Gennaro et al. does not disclose such a sharing of sources of randomness for use in computing. Gennaro et al. discloses a different kind of sharing for a different purpose. The sharing of Gennaro (on which the rejection is believed to be based) is the sharing of a secret key in the form of values related to -- but different from -- the key. A number of shares is required to obtain sufficient information to determine the key. None of the group members individually possesses sufficient information to know the key. In the sharing used to generate randomness in the embodiment of Fig. 1 of the pending application, each member of a group knows a value that is equal to the value known by other members. Each member knows the shared value. This is different from Gennaro, where a member's share is insufficient to know the key.

Furthermore, the shared value of the embodiment of Fig. 1 is used to index a pseudo random function to generate values useful for detecting misbehaving members of the group. This is a different motivation from threshold secret sharing of Gennaro, which shares values related to a key to avoid a single point of attack (or failure) of key material. While the members

of the group of the embodiment of Fig. 1 might also engage in a threshold sharing of a cryptographic key, that sharing would be a distinct aspect from knowing a shared value for generating randomness.

In light of the above remarks, it is believed the merit of this application will be appreciated and that the application will be passed to issuance. If, however, the Examiner is not persuaded, the applicants request an opportunity for a personal interview at the Examiner's earliest convenience.

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Assistant Commissioner for Patents, Washington, D.C. 20231"
on July 26, 2002
Signature Katie S. Lee
Typed or printed name
Katie S. Lee

Respectfully submitted,

Stuart T.F. Huang
Registration No. 34, 184
Steptoe & Johnson, LLP
1330 Connecticut Avenue, N.W.
Washington, DC 20036
Tel: (202) 429-8056
Fax: (202) 429-3902

VERSION WITH MARKINGS TO SHOW CHANGES

1. (Amended) A method of distributed cryptographic computation using a plurality of distributed electronic devices, said method comprising:

(a) computing shared values over a known and agreed context, each shared value being known by each member of [shared among] a distinct subset of the plurality of distributed electronic devices;

(b) at each of a plurality of the distributed electronic devices, generating a random value using said shared values;

(c) at each of a plurality of the distributed electronic devices, generating a partial result for the distributed cryptographic computation using at least one of said random values; and

(d) computing a final result for the distributed cryptographic computation using partial results.